REMARKS

Upon entry of the foregoing Amendment, claims 1-45 are pending in the application. Claims 1-5, 7, 9-16, 18-24, and 26-35 have been amended. No claims have been cancelled. Claims 36-45 have been newly added. Applicants believe that this Amendment does not add new matter. In view of the foregoing Amendment and the following Remarks, allowance of all the pending claims is requested.

REJECTION UNDER 35 U.S.C. § 103

A. CLAIMS 1-8, 10-14, 16-21, 23-28, AND 30-35

The Examiner has rejected claims 1-8, 10-14, 16-21, 23-28, and 30-35 under 35 U.S.C. § 103 as allegedly being unpatentable over U.S. Patent No. 6,772,345 to Shetty ("Shetty") in view of "An Adaptive Security Model for Mobile Agents in Wireless Networks" to Alampalayam et al. ("Alampalayam") and further in view of U.S. Patent Application Pub. No. 2004/0093521 to Hamadeh et al. ("Hamadeh"). This rejection is improper and should be withdrawn for at least the reason that the references relied upon, either alone or in combination, fail to disclose, teach, or suggest each and every feature of the claimed invention.

More particularly, Shetty, Alampalayam, and Hamadeh, either alone or in combination, disclose, teach, or suggest at least the feature of "monitoring the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitoring the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system," as recited in independent claim 1, for example.

In particular, Shetty generally relates to a system "for malware scanning of data that is being transferred or downloaded to a computer system" (Abstract). For example, Shetty describes protocol filters that "scan the traffic data stream for malwares" and "filter[] the malware out of the data stream" when detected (col. 3, lines 13-20). At best, scanning traffic data streams to detect and filter out malware in the manner described Shetty may relate to determining whether the data stream includes "one or more harmful computer codes." However, Shetty does not disclose, teach, or suggest that the protocol filter further scans the traffic data stream to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system."

Rather, Shetty indicates that when a protocol filter detects malware, the protocol filter filters the malware out of the stream and "then forwards the scanned data to workstation computer applications" (col. 4, lines 25-31). In other words, as the Examiner acknowledges on page 3 of the Office Action, "Shetty lacks adaptive signature creating technique" that would enable the protocol filters described therein to determine whether packets in an incoming data stream "include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system." Thus, for at least the reason that Shetty fails to disclose, teach, or suggest scanning a data stream to detect identifying information associated with previous attacks in addition to detecting malware (or "harmful computer code signatures"), Shetty fails to disclose, teach, or suggest at least the foregoing feature, as recited in independent claim 1. Alampalayam fails to cure this deficiency of Shetty for at least the following reasons.

Alampalayam generally relates to "a security framework that will detect automatically various attacks and then take appropriate measures to deal with the attack." However, Alampalayam does not disclose, teach, or suggest that such "appropriate measures" include "monitoring the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitoring the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system." In particular, although Alampalayam generally discusses the use of "adaptive security and holistic security," the security mechanism does not inspect information included in packets to determine whether the packets include "harmful computer code signatures" or "identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system."

Rather, the security mechanism described in Alampalayam is specifically characterized as "identifying . . . critical system parameters that are affected by various types of attacks" (Section 2.1). For example, Alampalayam states that "we could measure the relative change in parameter values and detect the type of attack," whereby the security model "uses measured vulnerability metrics and fuzzy logic to evaluate vulnerability". (Sections 2.1-2.2). Thus, instead of determining "whether one or more of the received packets include one or more harmful computer code signatures . . . [or] identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system," Alampalayam only monitors parameters associated with devices, not packets themselves, to determine whether the device "parameters change rapidly in a given time frame" (Section 2.2). For at least this reason, Alampalayam fails to disclose, teach, or suggest at least the foregoing feature, as recited in independent claim 1. Hamadeh fails to cure the foregoing deficiency of Shetty as well as this deficiency of Alampalayam for at least the following reasons.

Hamadeh generally relates to "tracing of packet flows back to a trusted point as near as possible to the flow in question" (Abstract). Although Hamadeh describes a system that attempts "to reconstruct the IP address of each border device that forwarded a particular packet flow into the trusted region," Hamadeh only performs such "traceback . . . while a [distributed denial-of-service] DDoS attack is on-going" (Abstract). In other words, Hamadeh does not use the reconstructed IP address information to determine "identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system," and then subsequently ""monitoring the received packets to determine whether one or more of the received packets include [the] identifying information.".

That is, Hamadeh specifically indicates that the system "will wait until enough fragments are received because the intrusion detection system requires quite a few packets (or fragments) that are malicious (i.e. part of a DDoS attack) to be able to determine that the server is under attack" (paragraph 0113). As such, because Hamadeh only processes a malicious packet flow after having entered a trusted region through a border device, Hamadeh does not disclose, teach, or suggest early detection of an attack by way of monitoring packets for "identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system." For at least this reason, Hamadeh fails to disclose, teach, or suggest at least the foregoing feature, as recited in independent claim 1.

Accordingly, for at least the foregoing reasons, Shetty, Alampalayam, and Hamadeh either alone or in combination, fail to disclose, teach, or suggest each and every feature of independent claim 1. The rejection is therefore improper and should be withdrawn.

Independent claims 10, 16, and 23 include features similar to those set forth in independent claim 1. Dependent claims 2-8, 11-14, 17-21, 24-28, and 30-35 depend from and add features to one of independent claims 1, 10, 16, and 23. Thus, the rejection of these claims is likewise improper and should be withdrawn for at least the same reasons.

B. CLAIMS 9, 15, 22, AND 29

The Examiner has rejected claims 9, 15, 22, and 29 under 35 U.S.C. § 103 as allegedly being unpatentable over Shetty in view of Alampalayam and Hamadeh and further in view of U.S. Patent Application Pub. No. 2002/0166063 to Lachman, III et al. ("Lachman"). This rejection is improper and should be withdrawn for at least the reason that the references relied upon, either alone or in combination, fail to disclose, teach, or suggest each and every feature of the claimed invention.

More particularly, for at least the reasons discussed above, Shetty, Alampalayam, and Hamadeh, either alone or in combination, do not disclose, teach, or suggest at least the feature of "monitoring the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitoring the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system," as recited in independent claim 1, for example. Lachman fails to cure at least this deficiency of Shetty, Alampalayam, and Hamadeh.

Accordingly, for at least the foregoing reasons, Shetty, Alampalayam, Hamadeh, and Lachman, either alone or in combination, fail to disclose, teach, or suggest each and every feature of independent claim 1. Independent claims 10, 16, and 23 include features similar to those set forth in independent claim 1. Dependent claims 9, 15, 22, and 29 depend from and add features to one of independent claims 1, 10, 16, and 23. Thus, the rejection of these claims is improper and should be withdrawn for at least the foregoing reasons.

NEW CLAIMS

For at least the reasons discussed above, the references relied upon, either alone or in combination, fail to disclose, teach, or suggest at least the feature of "monitoring the received packets to determine whether one or more of the received packets include one or more harmful computer code signatures, and further monitoring the received packets to determine whether one or more of the received packets include identifying information that has a history of being included in packets associated with one or more previous attacks directed at the target system," as recited in independent claim 1, for example.

Newly added claims 36-45 depend from and add features to independent claim 1. Thus, these claims are allowable over the references relied upon for at least the same reasons discussed above with respect to independent claim 1.

CONCLUSION

Having addressed each of the foregoing rejections, it is respectfully submitted that a full and complete response has been made to the outstanding Office Action. As such, the application is in condition for allowance. Notice to that effect is respectfully requested.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Date: **December 17, 2008**

Respectfully submitted,

By: ____________________
Syed Jafar Ali
Registration No. 58,780

PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. Box 10500
McLean, Virginia 22102
Main: 703-770-7900
Direct: 703-770-7540
Fax: 703-770-7901